



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,686	01/24/2002	Niels Rump	SCHO0093	3745
22862	7590	12/21/2007		
GLENN PATENT GROUP 3475 EDISON WAY, SUITE L MENLO PARK, CA 94025			EXAMINER HENNING, MATTHEW T	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 12/21/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/913,686

Applicant(s)

RUMP ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required, if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Art Unit: 2131

1 Regarding claim 1, Van Oorschot disclosed a method for producing a payload data
2 stream comprising a header and a payload data block containing encrypted payload data (See
3 Van Oorschot Fig. 3 X-fields, header fields, and encrypted message field), comprising the
4 following steps: generating a payload data key for a payload data encryption algorithm for
5 encrypting payload data (See Van Oorschot Col. 6 Lines 41-43 and Fig. 3 "Create low trust
6 symmetric key" K'); encrypting a first section of the payload data using said payload data key
7 and said payload data encryption algorithm to obtain an encrypted section of said payload data
8 block of said payload data stream (See Van Oorschot Col. 6 Lines 42-43 and Fig. 3 "Symmetric
9 encryption" and "encrypted message"), said first section including audio data, video data, a
10 combination of audio data and video data, text data or binary data forming an executable
11 program (See Van Oorschot Abstract), wherein a second section of the payload data remains
12 unencrypted (See Van Oorschot Col. 6 Lines 45-47 "public key of entity A"); processing the
13 unencrypted section of said payload data (See Van Oorschot Col. 6 Lines 45-50 "hash of X"
14 which contains the public key of A) to deduce information characterizing the unencrypted
15 second section of said payload data (See Van Oorschot Col. 6 Lines 49-60 $h_{40}(X)$); linking said
16 information and said payload data key by means of an invertible logic linkage to obtain a basic
17 value (See Van Oorschot Col. 6 Lines 56-60 " $K' \text{ XOR } h_{40}(X)$ "); encrypting said basic value
18 using a key of two keys being different from each other by an asymmetrical encryption method,
19 said two different keys being the public and the private keys respectively for said asymmetrical
20 encryption method, to obtain an output value being an encrypted version of said payload data key
21 (See Van Oorschot Col. 6 Line 60 – Col. 7 Line 7); and entering said output value into said
22 header of said payload data stream (See Van Oorschot Col. 6 Line 65 – Col. 7 Line 7 and Fig. 3

1 “A’s header field” and “B’s header field”), but Van Oorschot failed to disclose that the first and
2 second sections included audio data, video data, a combination of audio data and video data, or
3 binary data forming an executable program, or the X-fields containing audio data, video data, a
4 combination of audio data and video data, or binary data forming an executable program.

5 Nardone teaches that movie data needs to be protected from being copied and that this is
6 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further
7 that in order to save on processing cost, only portions of the movie data should be encrypted (See
8 Nardone Col. 1 Summary of the Invention).

9 Aucsmith teaches that public keys are provided in a digital certificates, and that digital
10 certificates enable anyone to authenticate the data within the certificate (See Aucsmith Abstract
11 and Background). Aucsmith further teaches that digital certificates can include multimedia data,
12 such as audio data, or video data, (See Aucsmith Col. 2 Lines 18-25), which may then be verified
13 and used to aid in verifying the owner of the certificate (See Aucsmith Col. 6 Line 25 – Col. 9
14 Line 60).

15 It would have been obvious to the ordinary person skilled in the art at the time of
16 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by
17 encrypting video data, and further by only encrypting portions of the video data. This would
18 have been obvious because the ordinary person skilled in the art would have been motivated to
19 protect movie data and to save on processing cost. It further would have been obvious to the
20 ordinary person skilled in the art at the time of invention to employ the teachings of Aucsmith in
21 the encryption system of Van Oorschot by providing the public key in a public key certificate in
22 the X-fields. This would have been obvious because the ordinary person skilled in the art would

Art Unit: 2131

1 have been motivated to provide the recipient with means to verify the authenticity of the public
2 key. Furthermore, it would have been obvious to the ordinary person skilled in the art to employ
3 the further teachings of Aucsmith by including multimedia data, such as audio or video data, in
4 the certificate. This would have been obvious because the ordinary person skilled in the art
5 would have been motivated to aid in verifying the owner of the certificate.

6 Regarding claim 17, Van Oorschot disclosed a method for decrypting an encrypted
7 payload data stream comprising a header and a payload data block containing a first section
8 having encrypted payload data (encrypted message), said first section including audio data, video
9 data, a combination of audio data and video data, text data, or binary data forming an executable
10 program (See Van Oorschot Abstract ciphertext), and a second section having unencrypted
11 payload data (public key of A), said header comprising an output value having been generated by
12 an encryption of a basic value by an asymmetrical encryption method using a key of two
13 different keys including a private and a public key, said basic value representing a linkage of a
14 payload data key, with which said first section having encrypted payload data is encrypted using
15 a payload data encryption algorithm, and information deduced by a certain processing of the
16 unencrypted second section of the payload data, said information characterizing a certain part of
17 said payload data stream unambiguously (See rejection of claim 1 above), said method
18 comprising the following steps: obtaining said output value from said header (See Van Oorschot
19 Fig. 4 "B's Header Field" and Col. 4 Lines 51-52); decrypting said output value using the other
20 key of said asymmetrical encryption method to obtain said basic value (See Van Oorschot Fig. 4
21 "private key decryption" and "B's high trust private key" and Col. 4 Lines 53-54); processing
22 the unencrypted second section of said payload data stream using the processing method used

1 when encrypting to deduce information characterizing the unencrypted second (See Van
2 Oorschot Fig. 4 “X-fields” and Col. 6 Lines 45-47); linking said information and said basic value
3 using the corresponding linkage as it has been used when encrypting to obtain said payload data
4 key (See Van Oorschot Fig. 4 “Unlevelling” and “X-fields” and Col. 4 Lines 54-56); and
5 decrypting the first section containing the encrypted payload data using said payload data key
6 and said payload data encryption algorithm used when encrypting (See Van Oorschot Fig. 4
7 “symmetric decryption” and “message”), but Van Oorschot failed to disclose that the first and
8 second sections included audio data, video data, a combination of audio data and video data, or
9 binary data forming an executable program, or the X-fields containing audio data, video data, a
10 combination of audio data and video data, or binary data forming an executable program.

11 Nardone teaches that movie data needs to be protected from being copied and that this is
12 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further
13 that in order to save on processing cost, only portions of the movie data should be encrypted (See
14 Nardone Col. 1 Summary of the Invention).

15 Aucsmith teaches that public keys are provided in a digital certificates, and that digital
16 certificates enable anyone to authenticate the data within the certificate (See Aucsmith Abstract
17 and Background). Aucsmith further teaches that digital certificates can include multimedia data,
18 such as audio data, or video data, (See Aucsmith Col. 2 Lines 18-25), which may then be verified
19 and used to aid in verifying the owner of the certificate (See Aucsmith Col. 6 Line 25 – Col. 9
20 Line 60).

21 It would have been obvious to the ordinary person skilled in the art at the time of
22 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by

Art Unit: 2131

1 encrypting video data, and further by only encrypting portions of the video data. This would
2 have been obvious because the ordinary person skilled in the art would have been motivated to
3 protect movie data and to save on processing cost. It further would have been obvious to the
4 ordinary person skilled in the art at the time of invention to employ the teachings of Aucsmith in
5 the encryption system of Van Oorschot by providing the public key in a public key certificate in
6 the X-fields. This would have been obvious because the ordinary person skilled in the art would
7 have been motivated to provide the recipient with means to verify the authenticity of the public
8 key. Furthermore, it would have been obvious to the ordinary person skilled in the art to employ
9 the further teachings of Aucsmith by including multimedia data, such as audio or video data, in
10 the certificate. This would have been obvious because the ordinary person skilled in the art
11 would have been motivated to aid in verifying the owner of the certificate.

12 Regarding claim 28, Van Oorschot disclosed a device for producing a payload data
13 stream comprising a header and a payload data block containing encrypted payload data (See
14 Van Oorschot Fig. 3 X-fields, header fields, and encrypted message field), comprising: a
15 generator for generating a payload data key for a payload data encryption algorithm for
16 encrypting payload data (See Van Oorschot Col. 6 Lines 41-43 and Fig. 3 "Create low trust
17 symmetric key" K'); a first encryptor for encrypting a first section of the payload data using said
18 payload data key and said payload data encryption algorithm to obtain an encrypted section of
19 said payload data block of said payload data stream (See Van Oorschot Col. 6 Lines 42-43 and
20 Fig. 3 "Symmetric encryption" and "encrypted message"), said first section including audio data,
21 video data, a combination of audio data and video data, text data, or binary data forming an
22 executable program (See Van Oorschot Abstract ciphertext); wherein a second section of the

1 payload data remains unencrypted (See Van Oorschot Col. 6 Lines 45-47 “public key of entity
2 A”); a processor for processing the unencrypted section of said payload data (See Van Oorschot
3 Col. 6 Lines 45-50 “hash of X” which contains the public key of A) to deduce information
4 characterizing the unencrypted second section of said payload data (See Van Oorschot Col. 6
5 Lines 49-60 $h_{40}(X)$); a linker for linking said information and said payload data key by means of
6 an invertible logic linkage to obtain a basic value (See Van Oorschot Col. 6 Lines 56-60 “K’
7 $XOR\ h_{40}(X)$ ”); a second encryptor for encrypting said basic value using a key of two keys being
8 different from each other by an asymmetrical encryption method, said two different keys being
9 the public and the private keys respectively for said asymmetrical encryption method, to obtain
10 an output value being an encrypted version of said payload data key (See Van Oorschot Col. 6
11 Line 60 – Col. 7 Line 7); and entering said output value into said header of said payload data
12 stream (See Van Oorschot Col. 6 Line 65 – Col. 7 Line 7 and Fig. 3 “A’s header field” and “B’s
13 header field”), but Van Oorschot failed to disclose that the first and second sections included
14 audio data, video data, a combination of audio data and video data, or binary data forming an
15 executable program, or the X-fields containing audio data, video data, a combination of audio
16 data and video data, or binary data forming an executable program.

17 Nardone teaches that movie data needs to be protected from being copied and that this is
18 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further
19 that in order to save on processing cost, only portions of the movie data should be encrypted (See
20 Nardone Col. 1 Summary of the Invention).

21 Aucsmith teaches that public keys are provided in a digital certificates, and that digital
22 certificates enable anyone to authenticate the data within the certificate (See Aucsmith Abstract

Art Unit: 2131

1 and Background). Aucsmith further teaches that digital certificates can include multimedia data,
2 such as audio data, or video data, (See Aucsmith Col. 2 Lines 18-25), which may then be verified
3 and used to aid in verifying the owner of the certificate (See Aucsmith Col. 6 Line 25 – Col. 9
4 Line 60).

5 It would have been obvious to the ordinary person skilled in the art at the time of
6 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by
7 encrypting video data, and further by only encrypting portions of the video data. This would
8 have been obvious because the ordinary person skilled in the art would have been motivated to
9 protect movie data and to save on processing cost. It further would have been obvious to the
10 ordinary person skilled in the art at the time of invention to employ the teachings of Aucsmith in
11 the encryption system of Van Oorschot by providing the public key in a public key certificate in
12 the X-fields. This would have been obvious because the ordinary person skilled in the art would
13 have been motivated to provide the recipient with means to verify the authenticity of the public
14 key. Furthermore, it would have been obvious to the ordinary person skilled in the art to employ
15 the further teachings of Aucsmith by including multimedia data, such as audio or video data, in
16 the certificate. This would have been obvious because the ordinary person skilled in the art
17 would have been motivated to aid in verifying the owner of the certificate.

18 Regarding claim 29, Van Oorschot disclosed a device for decrypting an encrypted
19 payload data stream comprising a header and a payload data block containing a first section
20 having encrypted payload data (encrypted message), said first section including audio data,
21 video data, a combination of audio data and video data, text data, or binary data forming an
22 executable program (See Van Oorschot Abstract ciphertext), and a second section having

Art Unit: 2131

1 unencrypted payload data (public key of A), said header comprising an output value having been
2 generated by an encryption of a basic value by an asymmetrical encryption method using a key
3 of two different keys including a private and a public key, said basic value representing a linkage
4 of a payload data key, with which said first section having encrypted payload data is encrypted
5 using a payload data encryption algorithm, and information deduced by a certain processing of
6 the unencrypted second section of the payload data, said information characterizing a certain part
7 of said payload data stream unambiguously (See rejection of claim 1 above), said device further
8 comprising: means for obtaining said output value from said header (See Van Oorschot Fig. 4
9 "B's Header Field" and Col. 4 Lines 51-52); a first decryptor for decrypting said output value
10 using the other key of said asymmetrical encryption method to obtain said basic value (See Van
11 Oorschot Fig. 4 "private key decryption" and "B's high trust private key" and Col. 4 Lines 53-
12 54); a processor for processing the unencrypted second section of said payload data stream using
13 the processing method used when encrypting to deduce information characterizing the
14 unencrypted second (See Van Oorschot Fig. 4 "X-fields" and Col. 6 Lines 45-47); a linker for
15 linking said information and said basic value using the corresponding linkage as it has been used
16 when encrypting to obtain said payload data key (See Van Oorschot Fig. 4 "Unlevelling" and
17 "X-fields" and Col. 4 Lines 54-56); and a second decryptor decrypting the first section
18 containing the encrypted payload data using said payload data key and said payload data
19 encryption algorithm used when encrypting (See Van Oorschot Fig. 4 "symmetric decryption"
20 and "message"), but Van Oorschot failed to disclose that the first and second sections included
21 audio data, video data, a combination of audio data and video data, or binary data forming an

Art Unit: 2131

1 executable program, or the X-fields containing audio data, video data, a combination of audio
2 data and video data, or binary data forming an executable program.

3 Nardone teaches that movie data needs to be protected from being copied and that this is
4 generally done through encrypting the movie data (See Nardone Col. 1 Lines 22-37), and further
5 that in order to save on processing cost, only portions of the movie data should be encrypted (See
6 Nardone Col. 1 Summary of the Invention).

7 Aucsmith teaches that public keys are provided in a digital certificates, and that digital
8 certificates enable anyone to authenticate the data within the certificate (See Aucsmith Abstract
9 and Background). Aucsmith further teaches that digital certificates can include multimedia data,
10 such as audio data, or video data, (See Aucsmith Col. 2 Lines 18-25), which may then be verified
11 and used to aid in verifying the owner of the certificate (See Aucsmith Col. 6 Line 25 – Col. 9
12 Line 60).

13 It would have been obvious to the ordinary person skilled in the art at the time of
14 invention to employ the teachings of Nardone in the encryption system of Van Oorschot by
15 encrypting video data, and further by only encrypting portions of the video data. This would
16 have been obvious because the ordinary person skilled in the art would have been motivated to
17 protect movie data and to save on processing cost. It further would have been obvious to the
18 ordinary person skilled in the art at the time of invention to employ the teachings of Aucsmith in
19 the encryption system of Van Oorschot by providing the public key in a public key certificate in
20 the X-fields. This would have been obvious because the ordinary person skilled in the art would
21 have been motivated to provide the recipient with means to verify the authenticity of the public
22 key. Furthermore, it would have been obvious to the ordinary person skilled in the art to employ

Art Unit: 2131

1 the further teachings of Aucsmith by including multimedia data, such as audio or video data, in
2 the certificate. This would have been obvious because the ordinary person skilled in the art
3 would have been motivated to aid in verifying the owner of the certificate.

4 Regarding claim 2, Van Oorschot, Nardone and Aucsmith disclosed that said payload
5 data encryption algorithm is a symmetrical encryption algorithm (See Van Oorschot Fig. 3
6 “symmetric encryption”).

7 Regarding claim 3, Van Oorschot, Nardone and Aucsmith disclosed that said invertible
8 logic linkage is self-inverting and includes an XOR- linkage (See Van Oorschot Col. 6 Lines 56-
9 60).

10 Regarding claim 4, Van Oorschot, Nardone and Aucsmith disclosed that one key of said
11 two keys being different from each other is the private key of a producer of said payload data
12 stream or the public key of a consumer of said payload data stream (See Van Oorschot Fig. 3 B’s
13 high trust public key).

14 Regarding claim 5, Van Oorschot, Nardone and Aucsmith disclosed that said part of said
15 payload data stream being processed to deduce said information includes at least a part of said
16 header (See Van Oorschot Fig. 3 “X-Field” and Col. 6 Lines 49-55).

17 Regarding claim 6 Van Oorschot, Nardone and Aucsmith disclosed that said step of
18 processing comprises forming a hash sum (See Van Oorschot Col. 6 Lines 49-55).

19 Regarding claim 7, Van Oorschot, Nardone and Aucsmith disclosed further comprising
20 the following step: identifying an algorithm being used in said step of processing by an entry into
21 said header (See Van Oorschot Abstract Lines 14-16).

1 Regarding claim 14 Van Oorschot, Nardone and Aucsmith disclosed that said step of
2 processing further comprises the following sub-step: setting said entry for said output value in
3 said header to a defined value and processing said entire header, including said entry set to a
4 defined value (See Van Oorschot Fig. 3 "X-Field" and Col. 6 Lines 49-55).

5 Regarding Claim 16, Van Oorschot, Nardone and Aucsmith disclosed the following step:
6 identifying said payload data encryption algorithm by an entry into said header of said payload
7 data stream (See Van Oorschot Abstract Lines 14-16).

8 Regarding claim 19, Van Oorschot, Nardone and Aucsmith disclosed that said part being
9 processed to deduce said information is said header (See Van Oorschot Fig. 4 "X-Fields").

10 Regarding claim 23, Van Oorschot, Nardone and Aucsmith disclosed that one key having
11 been used when encrypting is the public key of said asymmetrical encryption method, while the
12 other key having been used when decrypting is the private key of said asymmetrical encryption
13 method (See Van Oorschot Fig. 3 "B's high trust public key" and Fig 4 "B's high trust private
14 key").

15 Regarding claim 24, Van Oorschot, Nardone and Aucsmith disclosed that said step of
16 processing includes forming a hash sum (See Van Oorschot Col. 6 Lines 49-55 and Fig. 4
17 "Unlevelling").

18 Regarding claim 25, Van Oorschot, Nardone and Aucsmith disclosed that a part of said
19 header having been set to a defined value for said step of processing when encrypting is set to the
20 same defined value for said step of processing when decrypting (See Van Oorschot Fig. 3 "X-
21 fields" and Fig. 4 "X-fields" wherein they must be the same defined value because they were
22 both set by the sender upon sending).

1 Regarding claim 26, Van Oorschot, Nardone and Aucsmith disclosed that said part of
2 said header being set to a defined value includes said entry for said output value of said header
3 (See Van Oorschot Fig. 3 "B's header field" and Fig. 4 "B's header field" wherein they must be
4 the same defined value because they were both set by the sender upon sending).

5 Regarding claim 27, Van Oorschot, Nardone and Aucsmith disclosed that said step of
6 linking comprises using an XOR-linkage (See Van Oorschot Col. 6 Lines 56-60 and Col. 4 Lines
7 54-56 and Fig. 4 "Unlevelling").

8
9 Claims 8, 11-12, 18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable
10 over Van Oorschot, Nardone and Aucsmith as applied to claims 1 and 17 above, and further in
11 view of Matyas et al. (US Patent Number 5,200,999) hereinafter referred to as Matyas.

12 Van Oorschot, Nardone and Aucsmith disclosed a system for sending a message from a
13 sender to a receiver in which the message was encrypted using a key, the key was encrypted, and
14 then the key was sent to the receiver with the encrypted message (See Van Oorschot Abstract
15 and Fig. 3). Van Oorschot further disclosed decrypting the key, and using the key to decrypt the
16 message at the receiver (See Van Oorschot Abstract and Fig. 4). However, Van Oorschot,
17 Nardone and Aucsmith failed to disclose sending license data along with the key and message.

18 Matyas teaches that when sending a key, in order to authenticate the use of the key, and
19 the validity of the key, certain data (License data) should be placed in the header along with the
20 key. This data includes key type, key usage data (for history purposes), algorithm identifier,
21 algorithm-specific data, key start date/time, key expiration data/time, device identifier, user
22 identifier, key identifier, logical device identifier, and user-defined data (See Matyas Col. 13
23 Line 66 – Col. 14 Lines 60). Matyas further teaches that this information should be verified
24 prior to use of the key (See Matyas Col. 100).

25 It would have been obvious to the ordinary person skilled in the art at the time of
26 invention to employ the teachings of Matyas in the key and message sending system and method

Art Unit: 2131

1 of Van Oorschot, Nardone and Aucsmith by placing the license information, taught by Matyas,
2 in the header of the message and checking this information prior to allowing the key and
3 message to be decrypted. This would have been obvious because the ordinary person skilled in
4 the art would have been motivated to protect the interests of the sender of the message and to
5 ensure the security of the message.

6
7 Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of
8 Van Oorschot, Nardone, Aucsmith and Matyas as applied to claim 8 above, and further in view
9 of Klemba et al. (US Patent Number 5,710,814) hereinafter referred to as Klemba.

10 Van Oorschot, Nardone, Aucsmith and Matyas disclosed sending license data for
11 controlling the usage of a key and message, including usage history (See rejection of claim 8
12 above), but failed to disclose the data including how often the message could be decrypted.

13 Klemba teaches that license data can be used to control the number of uses of a
14 cryptographic function (See Klemba Col. 14 Lines 14-19).

15 It would have been obvious to the ordinary person skilled in the art at the time of
16 invention to employ the teachings of Klemba in the messaging system and method of Van
17 Oorschot, Nardone, Aucsmith and Matyas by using the license information to limit the number
18 of times the message could be decrypted. This would have been obvious because the ordinary
19 person skilled in the art would have been motivated to protect the interests of the sender of the
20 message as well as to protect the message against compromise.

21
22 Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination
23 of Van Oorschot, Nardone, Aucsmith and Matyas as applied to claim 8 above, and further in
24 view of Edenson et al. (US Patent Number 6,198,875) hereinafter referred to as Edenson.

1 Van Oorschot, Nardone, Aucsmith and Matyas disclosed sending license data for
2 controlling the usage of a key and message, including usage history (See rejection of claim 8
3 above), but failed to disclose the data including how often the message could be copied and how
4 often it had already been copied.

5 Edenson teaches that license information can include how many copies of licensed data
6 can be made (See Edenson Col. 4 Paragraph 2).

7 It would have been obvious to the ordinary person skilled in the art at the time of
8 invention to employ the teachings of Edenson in the messaging system of Van Oorschot,
9 Nardone, Aucsmith and Matyas by including information regarding the number of allowed
10 copies of the message that are permitted. This would have been obvious because the ordinary
11 person skilled in the art would have been motivated to protect the interests of the message
12 sender, and to protect the message itself from unauthorized distribution. Further, it would have
13 been necessary to also keep track of the number of copies already made in order to enforce the
14 copy limit.

15
16 Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination
17 of Van Oorschot, Nardone, Aucsmith and Matyas as applied to claim 8 above, and further in
18 view of Schneier ("Applied Cryptography Second Edition").

19 Van Oorschot, Nardone, Aucsmith and Matyas disclosed sending license data for
20 controlling the usage of a key and message, including usage history (See rejection of claim 8
21 above), but failed to disclose including the license in the hash function.

Art Unit: 2131

1 Schneier teaches that hashes are used to authenticate the data being hashed upon receipt
2 of the data in order to detect any unauthorized changes to the data (See Schneier Pages 30-31
3 Section 2.4).

4 It would have been obvious to the ordinary person skilled in the art at the time of
5 invention to employ the teachings of Schneier in the messaging system of Van Oorschot,
6 Nardone, Aucsmith and Matyas by hashing the License data along with the X-fields. This would
7 have been obvious because the ordinary person skilled in the art would have been motivated to
8 protect against undetected changes to the license data sent with the message.

9
10 Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot,
11 Nardone, and Aucsmith as applied to claim 1 above, and further in view of Roediger (US Patent
12 Number 4,899,333).

13 Van Oorschot, Nardone, and Aucsmith disclosed sending a message from a sender to a
14 receiver, including a header and a hash of the header (See Van Oorschot Col. 6), but Van
15 Oorschot failed to disclose including a sender identifier and a receiver identifier in the header, or
16 in the hash.

17 Roediger teaches that packet headers contain a source address (sender identifier) and a
18 destination address (recipient identifier) and that a checksum should include these fields in order
19 to ensure that the fields are not corrupted (See Roediger Col. 37 Lines 53-63).

20 It would have been obvious to the ordinary person skilled in the art at the time of
21 invention to employ the teachings of Roediger in the messaging system of Van Oorschot,
22 Nardone, and Aucsmith by including source and destination addresses in the header and

Art Unit: 2131

1 including these in the hash. This would have been obvious because the ordinary person skilled
2 in the art would have been motivated to provide means for routing the message from the sender
3 to the receiver and allowing the receiver to verify that it was the intended receiver of the
4 message.

5
6 Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot,
7 Nardone, and Aucsmith as applied to claim 17 above, and further in view of Schneier.

8 Van Oorschot, Nardone, and Aucsmith disclosed using a public key of the receiver for
9 encryption (See rejection of claim 23 above) but failed to disclose using a private key of an
10 asymmetrical key pair for encryption.

11 Schneier teaches that by encrypting data using a senders private key, the receiver can use
12 the senders public key to authenticate the sender of the data (See Schneier Pages 53-54).

13 It would have been obvious to employ the teachings of Schneier in the messaging system
14 of Van Oorschot, Nardone, and Aucsmith by encrypting the leveled key with the private key of
15 the sender and decrypting it with the public key of the sender. This would have been obvious
16 because the ordinary person skilled in the art would have been motivated to provide sender
17 authentication at the receiver.

18
19 Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot,
20 Nardone, and Aucsmith as applied to claims 28 and 29 above, and further in view of Kane et al.
21 (US Patent Number 5,315,635) hereinafter referred to as Kane.

Art Unit: 2131

1 Van Oorschot, Nardone, and Aucsmith disclosed sending messages from a sender to a
2 receiver (See Van Oorschot Abstract), but failed to disclose the sending being from a personal
3 computer to a personal computer.

4 Kane teaches that messages can be sent between personal computers (See Kane Col. 1
5 Lines 45-51).

6 It would have been obvious to the ordinary person skilled in the art at the time of
7 invention to employ the teachings of Kane in the messaging system of Van Oorschot, Nardone,
8 and Aucsmith by sending the encrypted messages from a sending personal computer to receiving
9 personal computer. This would have been obvious because the ordinary person skilled in the art
10 would have been motivated to protect messages sent between two personal computers.

11 *Conclusion*

12 Claims 1-30 have been rejected and claim 31 has been cancelled.

13 Applicant's amendment necessitated the new ground(s) of rejection presented in this
14 Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).
15 Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

16 A shortened statutory period for reply to this final action is set to expire THREE
17 MONTHS from the mailing date of this action. In the event a first reply is filed within TWO
18 MONTHS of the mailing date of this final action and the advisory action is not mailed until after
19 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period
20 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
21 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131


however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew Henning/
Assistant Examiner
Art Unit 2131
12/18/2007


AYAZ SHEKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100